

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Kazue SAKO
Title: ELECTRONIC TENDER SYSTEM
Appl. No.: Unknown
Filing Date: December 28, 1999
Examiner: Unknown
Art Unit: Unknown

UTILITY PATENT APPLICATION
TRANSMITTAL

Assistant Commissioner for Patents
Box PATENT APPLICATION
Washington, D.C. 20231

Sir:

Transmitted herewith for filing under 37 C.F.R. § 1.53(b) is the nonprovisional utility patent application of:

Kazue SAKO

Enclosed are:

- ☒ [X] Specification, Claim(s), and Abstract (15 pages).
- ☒ [X] Drawings (3 sheets, Figures 1-3).
- ☒ [X] Declaration and Power of Attorney (2 pages).
- ☒ [X] Assignment of the invention to NEC CORPORATION.
- ☒ [X] Assignment Recordation Cover Sheet.
- ☒ [X] Check in the amount of \$40.00 for Assignment recordation.
- ☐ [] Small Entity statement.
- ☐ [] Information Disclosure Statement.
- ☐ [] Form PTO-1449 with copies of ___ listed reference(s).

The filing fee is calculated below:

	Claims as Filed	Included in Basic Fee	Extra Claims	Rate	Fee Totals
Basic Fee				\$760.00	\$760.00
Total Claims:	8	- 20	= 0	x \$18.00	= \$0.00
Independents:	1	- 3	= 0	x \$78.00	= \$0.00
If any Multiple Dependent Claim(s) present:			+	\$260.00	= \$0.00
				SUBTOTAL:	= \$760.00
				Assignment recordation fee:	= \$40.00
				TOTAL FILING FEE:	= \$800.00

- ☒ A check in the amount of \$800.00 to cover the filing fee is enclosed.
- ☐ The required filing fees are not enclosed but will be submitted in response to the Notice to File Missing Parts of Application.
- ☒ The Assistant Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Assistant Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741.

Please direct all correspondence to the undersigned attorney or agent at the address indicated below.

Respectfully submitted,

Date December 28, 1999

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

By Phillip J. Artiola *Reg. No.*
38,819
for / David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

ELECTRONIC TENDER SYSTEM

Background of the Invention:

The present invention relates to an electronic tender
5 system, and particularly a method for coding the bidding price
and a method for deciding the contract price.

As known from Japanese Patent Laid-Open No.HEI2-
118876, for example, such electronic tender system adopts a
coding technology, because the bidding price information
10 should be kept secret generally until the tender opening. The
coded bidding price information is decoded all at once at the
tender opening, to decide the highest or the lowest bidding
price among them as the contract price. There, the
announcement of all bidding prices allows to everyone to
15 confirm that the contact price has been decided correctly, in
other words, it was the highest or the lowest price among the
bidding prices.

Recently, it is demanded not to publish the bidding price
not accepted as the contact price, in view of the privacy
20 protection. To meet this requirement, for example, an
approach has been disclosed in an article, "Multi-round
Anonymous Auction Protocols" by Kikuchi, Harkavy and Tyger,
published in "IEEE Workshop on Dependable and Real-time
E-Commerce System". This approach disclosed in the prior art
25 literature is shown in Fig. 1.

In this approach, the bidder creates a data row
corresponding to his bidding price and encodes each data
respectively. The opener receives code string data transmitted

2

by all bidders, integrates and then decodes them to decide the contract price. In this approach, as the code string data of individual bidder is not decoded, the bidding price of respective bidder can be kept secret, and at the same time, the identification information of the highest price bidder can be extracted, by integrating code string data of all bidders.

Now, the principle of identification extraction will be described. A bidder having an identification information ID_i , creates a data row corresponding to his bidding price as follows. Suppose the tender reception range be (a, b) and his bidding price $a + v$ ($< b$), then $(v + 1)$ times $\times ID_i$ are enumerated. Next, 0 are enumerated $b - (a + v)$ times. Thus, a data row containing $(b - a + 1)$ elements is generated.

A data row where respective elements of the data row are added by each element is output, by integrating data rows from all bidders generated in this way. In this data row, suppose the element where 0 appears first be t th, the highest bidding price (contract price) is $a + t - 1$, and the bidder who has the identification information indicated by the price of the $t - 1$ st element.

However, in this prior art, the bidding data becomes longer in proportion to the tender reception price range, because the data row is created in proportion to the length of the tender reception range, and then it is divided to code. Further, when a plurality of bidders have offered the contract price, it is impossible to determine the identification or the number of concerned bidders, because the decoding result of the $t - 1$ st element is the sum of ID information of bidders of

2

3

the corresponding bidding price.

Summary of the Invention:

It is therefore an object of the present invention to provide an electronic tender system, allowing to reduce the bidding data, and at the same time, to identify the concerned bidder even when a plurality of bidders have offered the contract price, and moreover, to keep secret the bidding information of other bidding prices than that of the successful bidder.

Other objects of the present invention will become clear as the description proceeds.

The electronic tender system according to the present invention is characterized by that a code parameter depending on the bidding price is delivered to the coding function section in its bidder sub-system, and, a contract price candidate selection function, and a retrieve function by the decode parameter depending on the candidate price are provided, in order to decide the contract price in its tender opening sub-system.

The introduction of these code parameter and decode parameter realizes an effect to judge only if the bidding price is identical to the contract price candidate. Therefore, the highest or the lowest bidding price and its bidder can be decided, by judging if there is a bidding price identical to the contract price candidate, changing the contract price candidate one by one from the tender possible highest price or the lowest price, and further, how the other bidders have tendered can be concealed.

3

Brief Description of the Drawings:

Fig. 1 is a block diagram for showing a conventional method;

Fig. 2 is a block diagram for showing a composition of
5 the present invention; and

Fig. 3 is a block diagram for showing a composition of the retrieve means of the present invention.

Detailed Description of the Preferred Embodiments:

Referring now to Figs. 2 and 3, description will proceed
10 to an electronic tender system according to a preferred embodiment of the present invention.

Fig. 2 is a block diagram showing an embodiment of the present invention. The electronic tender system according to the present invention comprises a bidder sub-system 100 and a tender opening sub-system 200. The bidder sub-system 100 includes a code parameter acquisition means 101 and a coding means 102, while the tender opening sub-system 200 includes a reception means 201, a contract price candidate selection means 202, a decode parameter acquisition means 203 and a
15 retrieve means 204.

The retrieve means 204 includes, as shown in Fig. 3, a decoding means 205 and a judgement means 206, and the decoding means 205 decodes sequentially coded bidding prices received by the reception means 201 based on the decode
20 parameter acquired by the decode parameter acquisition means 205, while the judgement means 206 judges that the coded bidding price is identical to the contact price candidate selected by the selection means 202, in the case when the

decoding result by the decoding means 205 becomes a fixed value.

Note that, in this embodiment, to simplify the description, it is supposed, hereinafter, that a bidder sub-system that has offered the highest price, among bid prices, will be decided as the successful bidder, though it is similar in the case where the lowest price will be the contract price.

The input to the bidder sub-system 100, is the bidding price desired by this the bidder sub-system. The bidding price bid in this bidder sub-system 100 is delivered to the code parameter acquisition means 101. In the code parameter acquisition means 101, the code parameter necessary for the coding means 102 depending on this bidding price is acquired and delivered to the coding means 102. The coding means 102 performs the coding operation based on the supplied code parameter, and delivers the coded bidding data to the transmission means 103. The transmission means 103, transmits the coded bidding data to the reception means 201 of the tender opening sub-system 200.

The reception means 201 of the tender opening sub-system 200, receives the coded bidding data sent from respective bidder sub-system 100, directs the contract price selection means 202 to start the tender opening on the tender opening day. The contract price selection means 202 directed to open the tender, first, takes the highest price within the acceptable range the candidate price, and supplied the decode parameter acquisition means 203 with this candidate price.

The decode parameter acquisition means 203, acquires

this decode parameter depending on this candidate price, and delivers to the retrieve means 204. The retrieve means 204, decodes all coded bidding data received using the supplied decode parameter, in the decoding means 205, and retrieves if
5 there is a bidding price same as the candidate price among the coded bidding data by the judgement means 206. If it is the case, the bidder sub-system that has sent that coded bidding data will be accepted. If there is no coded bidding data created taking this candidate price as bidding price, the retrieve
10 means 204, outputs that the concerned candidate price is not the contract price to the contract price selection means 202.

Upon the reception of a non candidate signal from the retrieve means 204, the contract price selection means 202, takes the next lower price than the current candidate price as
15 a new candidate price, and delivers it to the decode parameter acquisition means 203. Then, the similar operation will be repeated until the judging means 206 decides a successful bidder, or the candidate price becomes lower than the tender possible range. If the candidate price becomes lower than the
20 tender possible range, it is judged that no bidding is accepted, and this result is output before terminating the processing.

Now, as an example of this embodiment, the case where El Gamal code is used as coding function will be described. The El Gamal code being well known by those skilled in the art and
25 irrelevant to the present invention, its detailed explanation will be omitted.

First, the tender opening system creates a large prime p and a generator g . Besides, it decides a secret key x (v), a

public key $y(v)$ and a constant $M(v)$ for respective bidding price v . Here, the secret key $x(v)$ and the public key $y(v)$ present the following relation. $M(v)$ may be an arbitrary value, and for example, v and its hash value can be linked as $M(v)$, or it well may be a constant independent of v . As code parameters, $M(v)$ and $y(v)$ are adopted and as decode parameter $x(v)$. The code parameters are published, while the decode parameters are severely controlled in the tender opening sub-system.

The bidder sub-system 100, obtains code parameters, $M(v)$ and $y(v)$, for a bidding price v it desires, and codes $M(v)$ with the public key $y(v)$ based on the El Gamal code. The El Gamal code, belonging to the code type called probabilistic encryption, is known to produce a different coded message even if the same $M(v)$ is coded. The bidder sub-system 100, send this coding result to the tender opening system 200 as coded bidding data $C(v)$.

The tender opening sub-system 200 obtains a decode parameter $x(v')$ for a contract price candidate v' and decodes $C(v)$ using this decode parameter as secret key. There, if $v = v'$, obviously the decoding result will be $M(v) = M(v')$. On the contrary, if $v \neq v'$, the decoding result will hardly be $M(v')$. Thus, without obtaining the bidding price, it can be judged if it is equal to the contract price candidate.

If the contract price is decided to be v , all offered code bidding prices, and the decode parameter $x(v)$ corresponding the bidding possible price equal to or larger than v are published by the announcement means. Therefore, everyone can verify that there was no bidding price larger than v and

8

who has bid the contract price, as they can try to decode all offered code bidding prices using this announced decode parameter.

On the other hand, bidding prices inferior to the contract price can be concealed, as the decode parameter $x(v)$ corresponding to the bidding prices inferior to the contract price is not published. Further, problems in the case where a plurality of successful bidders exist as in the conventional method will not occur, because all bidding sub-systems will be identified, even when obviously a plurality of bidding sub-systems have offered the contract price.

As a specific embodiment, now a case where RSA code is used for coding function will be described. The detailed description of RSA code will be omitted as it is well known by those skilled in the art and not relevant to the present invention. For RSA coding, code parameter $y(v)$ is generated automatically from the bidding price v , without table lookup, and moreover, the fixed value $M(v)$ to be coded may not be fixed for all bidders.

First, the tender opening system generates large primes p and q , and supposes n their product. The bidder sub-system generates as follows the code parameter $M(v)$, $y(v)$, for the bidding price v it wishes. That is to say, it generates random numbers, and makes $M(v)$ be the concatenation of v , and this random number, and the hash value where they are coupled. Next, supposing $y(v)$, 1 is concatenated with the hash value of v , making it prime to $(p-1)(q-1)$ each other.

Then, $M(v)$ is codified with the public key $y(v)$ based on

8

RSA code of the modulus n . In this case, as different random numbers are generated for respective bidder, different coded messages are generated even if a same v is coded. The bidder sub-system transmits this coding result to the tender opening system 200 as coded bidding data $C(v)$.

The tender opening system 200 calculates $y(v')$ for a contract price candidate v' , namely it hash value, and calculates $x(v')$ that is the inverse element of $y(v')$ in the modulus $(p-1)(q-1)$, as decode parameter. Then, $C(v)$ is decoded in the modulus n taking this code parameter as secret key.

Here, if $v = v'$, obviously, the decoding result $M(v')$ will be a correct format by v' and a certain random number. On the other hand, if $v \neq v'$, the decoding result will hardly be such format. Thus, without obtaining the bidding price it-self, it can be judged if it is equal to the contract price candidate.

If the contract price is decided to be v , all offered code bidding prices, and respective result of decoding by the decode parameter $x(v)$ corresponding the tender possible price equal to or larger than v are published by the announcement means. Therefore, everyone can verify that there was no bidding price larger than v and who has bid the contract price, as they can confirm that the result coded by the code parameter $y(v')$ corresponding to the contact price candidate is equal to offered respective code bidding prices, using this announced decode parameter.

On the other hand, bidding prices inferior to the contract price can be concealed, as the decoding result

10

corresponding to the bidding prices inferior to the contract price is not published. Further, problems in the case where a plurality of successful bidders exist as in the conventional method will not occur, because all bidding sub-systems will be identified, even when obviously a plurality of bidding sub-systems have offered the contract price.

Moreover, it is assured that code bidding prices to be input into the tender opening system excludes those outside the bidding period, by publishing code bidding prices received before the bidding deadline, and opening only those published ones. As it is irrelevant to the present invention, the detailed description thereof will be omitted.

Additionally, it can be assured that the tender opening system will not decode illegally the code bidding price, by controlling or generating the decode parameter with a plurality of sub-systems, using distributed secret or group decryption technology or the like. As it is also irrelevant to the present invention, the detailed description thereof will be omitted.

Beside, a digital signature of the code bidding price can be added, in order to prevent the bidder bidding in the name of the other, or denying later the transmitted code bidding price; however, as it is also irrelevant to the present invention, the detailed description thereof will be omitted.

In this embodiment, to simplify, the case where a bidding sub-system that has offered the highest price, among bid prices, will be decided as the successful bidder has been described in detail; however, similarly, it can easily be applied

10

11

to the case wherein the lowest price will be the contract price, or to the case wherein a plurality of bidding sub-system that have offered a bidding price close to the highest price or the lowest price.

5 It is to be understood that the present invention is not limited to the aforementioned respective embodiments, and obviously, the respective embodiments can be executed by conveniently modifying them, without departing from the technical concept of the present invention.

10 As described hereinbefore, according to the present invention, it is possible to provide an electronic tender system, allowing to select the bidder who has offered the highest or the lowest price as successful bidder and moreover, to keep secret the bidding information of other bidding prices than that of
15 the successful bidder, based on a basic composition wherein the bidder sub-system codes by means of a code parameter depending on the bidding price, and the tender opening system decodes by a decode parameter depending on the contract price candidate.

11

What is claimed is :

1. An electronic tender system for accepting as contract price the highest or lowest price among bidding prices offered by a plurality of tenders, comprising :

5 a bidder sub-system including a code parameter acquisition means for taking as input a bidding price selected by the tender bidding subsystem within the tenderable range, and for acquiring a code parameter depending on the bidding price, a code processing means for using the code parameter obtained by said code parameter acquisition means, and a
10 transmission means for sending a coded message coded by said coding means to a tender opening sub-system, and

a tender opening sub-system including a reception means for accepting said coded bidding prices until the closing day, a selection means for selecting sequentially a contract
15 price candidate from the highest or the lowest among acceptable bidding prices, a decode parameter acquisition means for acquiring a decode parameter corresponding to the contract price candidate selected by said selection means, and
20 a retrieve means for retrieving if a same bidding price as the contract price candidate selected by said selection means exists among coded bidding prices accepted by said reception means using said decode parameter.

2. The electronic tender system as claimed in claim 1, wherein the code processing means of said bidder sub-system,

18

codes a fixed value using the code parameter obtained by said
code parameter acquisition means, and the retrieve means of
5 said tender opening sub-system includes a decoding means for
sequentially decoding coded bidding prices received by said
reception means according to the decode parameter acquired
by said decode parameter acquisition means, and a judgement
means for judging that the coded bidding price is identical to
10 the contact price candidate selected by said selection means in
the case where the decoding result becomes said fixed value.

3. The electronic tender system as claimed in claim 1,
wherein the code processing means of said bidder sub-system,
includes a coding operation of the fixed price by a public key
corresponding to said bidding price, and the decoding means of
5 said tender opening system, includes a decoding operation
with a secret key corresponding to said public key
corresponding to the contact price candidate.

4. The electronic tender system as claimed in claim 2,
wherein the code processing means of said bidder sub-system,
includes a coding operation of the fixed price by a public key
corresponding to said bidding price, and the decoding means of
5 said tender opening system, includes a decoding operation
with a secret key corresponding to said public key
corresponding to the contact price candidate.

5. The electronic tender system as claimed in claim 1,
wherein said tender opening system includes an announcement

13

means for announcing a portion of decode parameter acquired
in the decode parameter acquisition means or decoding results
5 obtained in the retrieve means for each contact price
candidate.

6. The electronic tender system as claimed in claim 2,
wherein said tender opening system includes an announcement
means for announcing a portion of decode parameter acquired
in the decode parameter acquisition means or decoding results
5 obtained in the retrieve means for each contact price
candidate.

7. The electronic tender system as claimed in claim 3,
wherein said tender opening system includes an announcement
means for announcing a portion of decode parameter acquired
in the decode parameter acquisition means or decoding results
5 obtained in the retrieve means for each contact price
candidate.

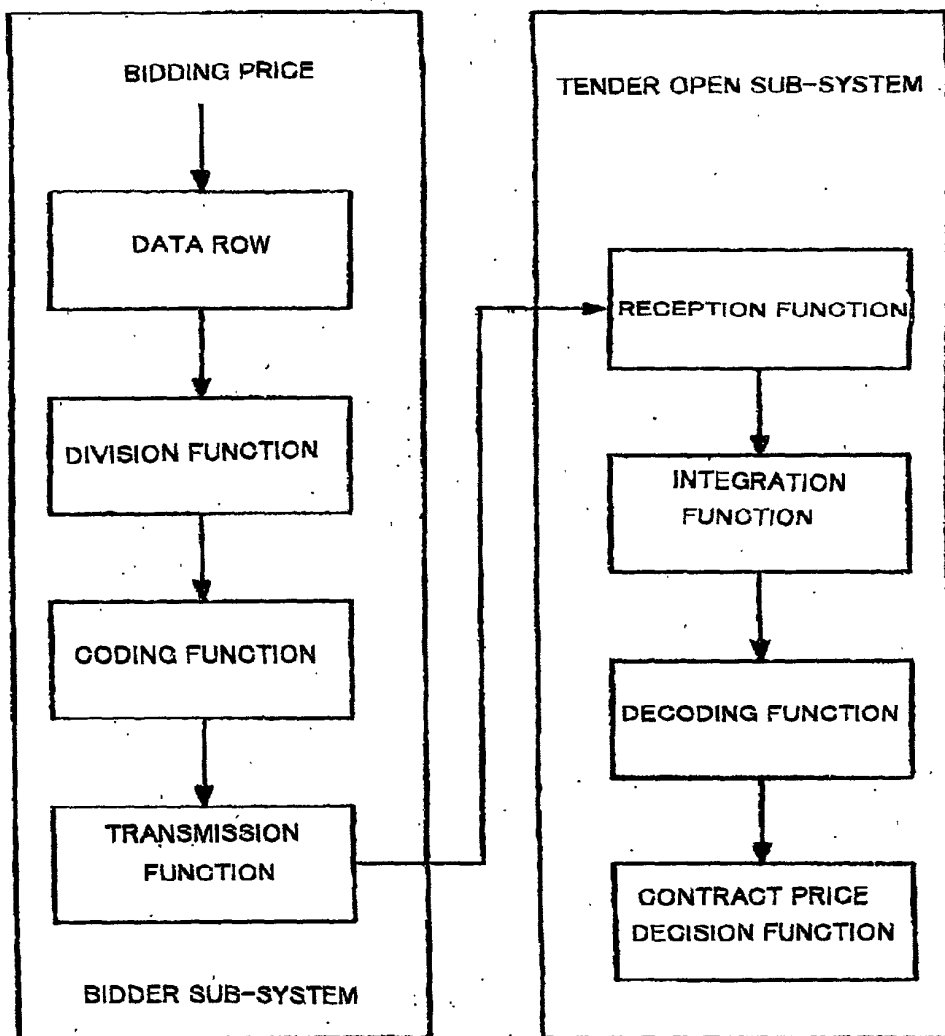
8. The electronic tender system as claimed in claim 4,
wherein said tender opening system includes an announcement
means for announcing a portion of decode parameter acquired
in the decode parameter acquisition means or decoding results
5 obtained in the retrieve means for each contact price
candidate.

15

Abstract of the Disclosure:

The coding function section in the bidder sub-system 100 is supplied with a code parameter depending on the bidding price, and the bidding price is coded depending on this code parameter. The tender opening system 200 decodes sequentially the decode parameter corresponding to the highest bidding price starting from the highest or the lowest one among bidding prices that can possibly be accepted, and the one that is successfully decoded is judged to be a bidding price corresponding to that parameter and accepted as contract price. The information of unaccepted bidding prices will be concealed, by not publishing the decode parameter concerning the bidding prices of the order inferior to the contract price.

15



(PRIOR ART)
FIG 1

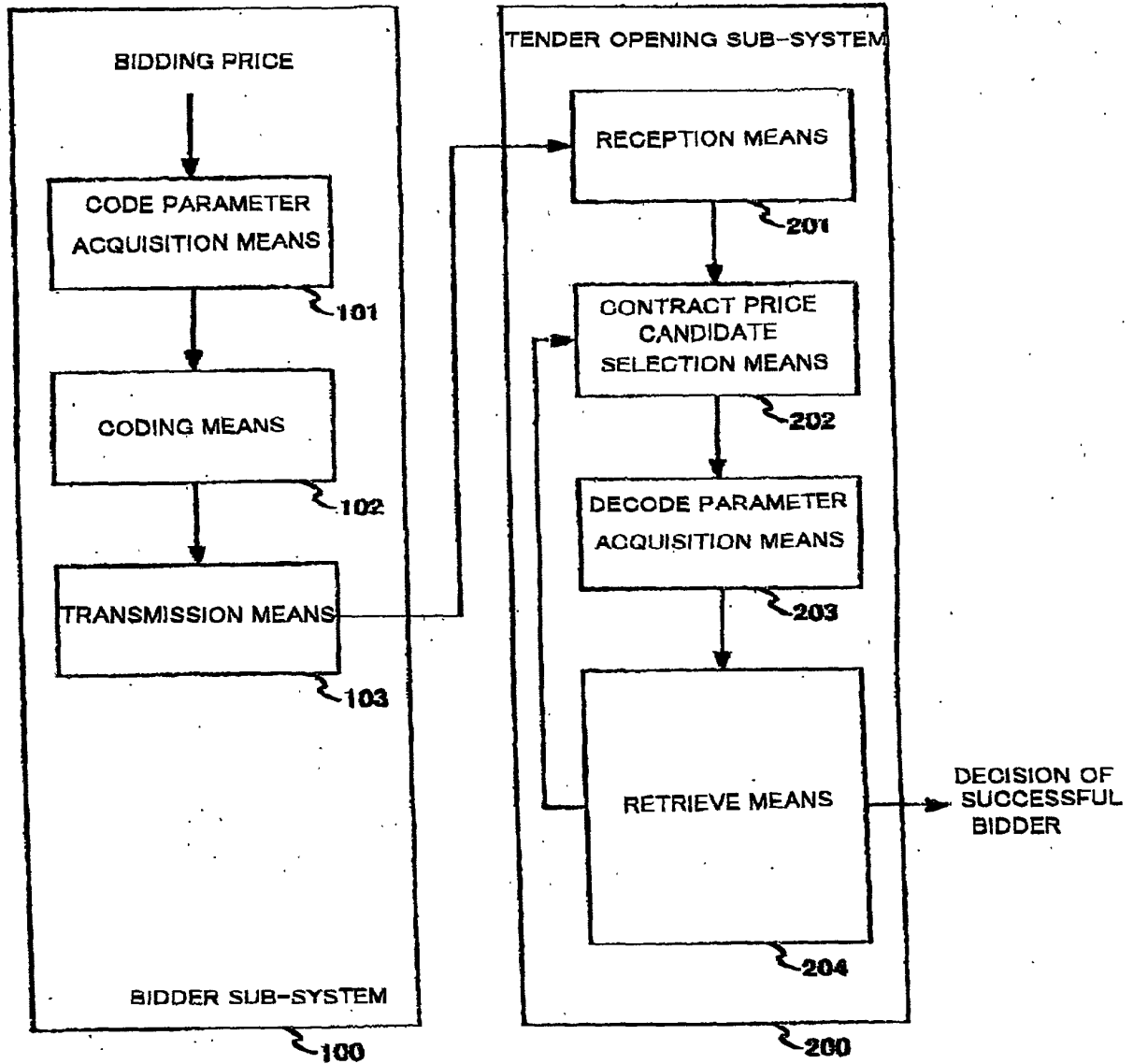


FIG 2

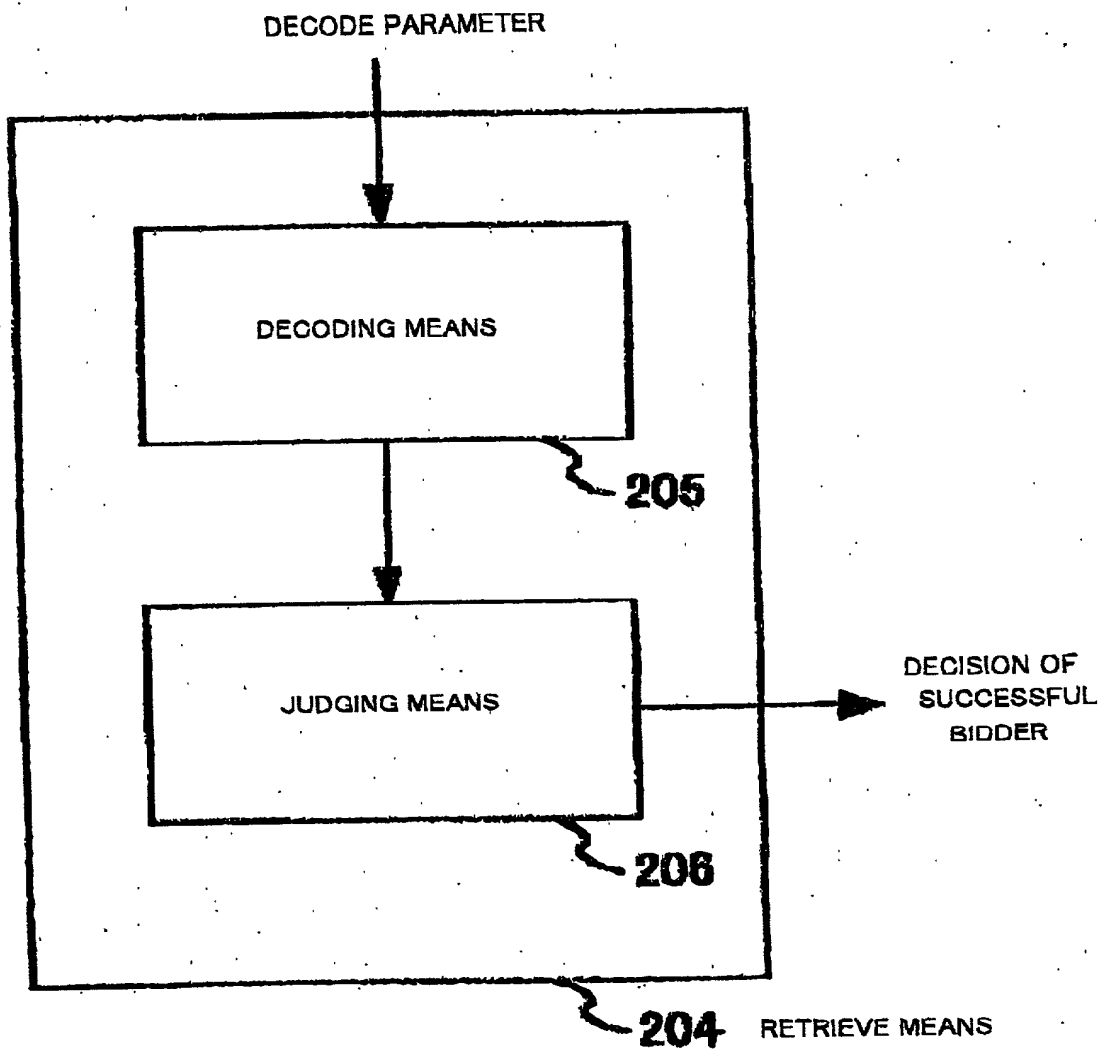


FIG 3

Docket No. _____

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

ELECTRONIC TENDER SYSTEM

the specification of which is attached hereto unless the following box is checked:

☐ was filed on _____ as United States Application Number or PCT International Application Number _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is known by me to be material to patentability as defined in Title 37, Code of Federal Regulations § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

NUMBER	COUNTRY	DAY/MONTH/YEAR FILED	PRIORITY CLAIMED
0-374833	Japan	28/12/1998	Yes

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

APPLICATION NO.	FILING DATE

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is known by me to be material to patentability as defined in Title 37, Code of Federal Regulations § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

APPLICATION SERIAL NO.	FILING DATE	STATUS: PATENTED, PENDING, ABANDONED

I hereby appoint as my attorneys, with full powers of substitution and revocation, to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: Stephen A. Bent, Reg. No. 29,768; David A. Blumenthal, Reg. No. 26,257; John J. Feldhaus, Reg. No. 28,822; Donald D. Jeffery, Reg. No. 19,980; Eugene M. Lee, Reg. No. 32,039; Peter G. Mack, Reg. No. 26,001; Brian J. McNamara, Reg. No. 32,789; Sybil Meloy, Reg. No. 22,749; George E. Quillin, Reg. No. 32,792; Colin G. Sandercock, Reg. No. 31,298; Bernhard D. Saxe, Reg. No. 28,665; Charles F. Schill, Reg. No. 27,390; Richard L. Schwaab, Reg. No. 25,479; Arthur Schwartz, Reg. No. 22,115; Harold C. Wegner, Reg. No. 25,238.

PAGE 2

Docket No. _____

Address all correspondence to FOLEY & LARDNER, Washington Harbour, 3000 K Street, N.W., Suite 500, P.O. Box 25696, Washington, D.C. 20007-8696. Address telephone communications to _____ at (202) 672-5300.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of First or Sole Inventor KAZUE SAKO	Signature of First or Sole Inventor <i>Kazue Sako</i>	Date December 27, 1999
Residence Address Tokyo, Japan	Country of Citizenship Japan	
Post Office Address c/o NEC Corporation, 7-1, Shiba 5-chome, Minato-ku, Tokyo, Japan		

Full Name of Second Inventor	Signature of Second Inventor	Date
Residence Address	Country of Citizenship	
Post Office Address		

Full Name of Third Inventor	Signature of Third Inventor	Date
Residence Address	Country of Citizenship	
Post Office Address		

Full Name of Fourth Inventor	Signature of Fourth Inventor	Date
Residence Address	Country of Citizenship	
Post Office Address		

Full Name of Fifth Inventor	Signature of Fifth Inventor	Date
Residence Address	Country of Citizenship	
Post Office Address		